AN ACT TO PROTECT STUDENT PRIVACY WITH
RESPECT TO PERSONAL ELECTRONIC DEVICES ON CAMPUS

Be it enacted by the {fill in appropriate language for your state}:

Section 1 – Definitions: For the purposes of this Act:

(A) "1-to-1 device" shall mean a technological device provided to a student pursuant to any program authorized by an educational institution where the technological device is provided to a student by or through an educational institution for overnight or at-home use.

(B) "Educational institution" shall mean:

(1) A private or public school, institution or school district, or any subdivision thereof, that offers participants, students or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school employees acting under the authority or on behalf of an educational institution; or

(2) A state or local educational agency authorized to direct or control an entity in Section 1(F)(1).

(C) "Educational record" shall mean educational record as defined by 20 U.S.C. §1232g(a)(4) on the date of this Act's adoption.

(D) "Education research" shall mean the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

(E) "Law enforcement official" shall mean an officer or employee of any agency or authority of the {state/commonwealth} of {State name}, or a political subdivision or agent thereof, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, make arrests, and/or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(F) "Personal technological device" shall mean a technological device owned, leased, or otherwise lawfully possessed by a student that is not a 1-to-1 device.

Comment [CM1]: *NOTE TO AFFILIATES: Delete this definition if your state does not have law governing data privacy on 1-to-1 devices, or if this bill is not is being combined with a 1-to-1 device privacy bill.*

Comment [CM2]: *NOTE TO AFFILIATES: Your state may already have a definition of this term, and you may opt to use that definition instead. This model bill was drafted in October 2015.*

Comment [CM3]: *NOTE TO AFFILIATES: Your state may already have a definition of this term, but **make sure** it includes state and local officers, but not federal.*

Comment [CM4]: *NOTE TO AFFILIATES: Delete this language ("*that is not a 1-to-1 device") *if your state does not have a law governing data privacy on 1-to-1 devices, or if this bill is not being combined with a 1-to-1 device privacy bill.*

(G) "School employee" shall mean an individual who is employed by an educational institution, compensated through an annual salary or hourly wage paid by an educational institution, and whose services are primarily rendered at a physical location which is owned or leased by that educational institution. For purposes of this Act, individuals with law enforcement or school security responsibilities, including school resource officers, school district police officers, contract or private security companies, security guards, or other law enforcement personnel are not school employees.

Comment [CM5]: *NOTE TO AFFILIATES: Your state may already have a definition of this term.*

(H) "Student" shall mean any student, participant or trainee, whether full-time or part-time, in an organized course of study at an educational institution.

Comment [CM6]: *NOTE TO AFFILIATES: Your state may already have a definition of this term.*

(I) "Technological device" shall mean any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

Section 2 – Student's Personal Electronic Devices on Campus:

(A) No school employee may access, or compel a student to produce, display, share or provide access to, any data or other content input into, stored upon, or accessible from a student's personal technological device, even where the personal technological device is being carried or used in violation of an educational institution policy.

(B) Notwithstanding Section 2(A), a school employee may search a student's personal technological device, if:

(1) The school employee has a reasonable suspicion that a student has violated or is violating an educational institution policy and that the student's personal technological device contains evidence of the suspected violation. In such cases, the school employee may search the student's personal technological device if:

(a) The student's personal technological device is located on the property of the educational institution;

(b) Prior to searching a student's personal technological device, the school employee:

(i) Documents the reasonable individualized suspicion giving rise to the need for the search; and

(ii) Notifies the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation.

a. An educational institution, subject to any other relevant legal restrictions, may seize a student's personal technological device to prevent data deletion pending notification, provided that:

i. The pre-notification seizure period is no greater than 48 hours; and

ii. The personal technological device is stored securely on educational institution property and not accessed during the pre-notification seizure period.

(c) The search is strictly limited to finding evidence of the suspected policy violation; and

(d) The school employee immediately ceases searching the student's personal technological device upon finding sufficient evidence of the suspected violation.

(e) It shall be a violation of this subsection to copy, share, or transfer any data, or any information thereabout, that is unrelated to the specific suspected violation which prompted the search of the student's personal technological device.

(2) Doing so is necessary in response to an imminent threat to life or safety.

(a) Within 72 hours of accessing a personal technological device in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data was accessed.

(C) Notwithstanding Section 2(B)(1), where a student is suspected of illegal conduct, no search of the student's personal technological device may occur unless a judicial warrant authorizing a law enforcement official to search the student's personal electronic device has been secured, even if the student is also suspected of a related or unrelated violation of an educational institution policy.

Section 3 – Limitations on Use:

(A) Evidence or information obtained or collected in violation of this Act shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

Section 4 – Penalties:

(A) Any person or entity who violates this Act shall be subject to legal action for damages and/or equitable relief, to be brought by any other person claiming a violation of this Act has injured his or her person or reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of this Act, and a reasonable attorney's fee and other costs of litigation.

(B) Any school employee who violates this Act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Section 5 – Severability:

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 8 – Effective Date:

This Act shall take effect upon passage.